

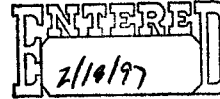


JAMES D. McLAUGHLIN
DIRECTOR
AGENCY RELATIONS
TRUST AND SECURITIES

1120 Connecticut Avenue, N.W.
Washington, D.C. 20036
(202) 663-5324

February 13, 1997

Ms. Nancy Crow
Regulatory Policy Division
Bureau of Export Administration
Department of Commerce
14th Street and Pennsylvania Ave., NW
Room 2705
Washington, D.C. 20230
HAND DELIVERED



RE: Encryption Items Transferred from the U.S. Munitions List to the
Commerce Control List ; 61 Federal Register 68572, December 30, 1996

Dear Ms. Crow:

The American Bankers Association (ABA) is pleased to respond to the Department of Commerce's Interim-Final Cryptographic Export Control Regulation Amendments. The American Bankers Association brings together all elements of the banking community to best represent the interests of this rapidly changing industry. Its membership -- which includes community, regional, and money center banks and holding companies, as well as savings associations, trust companies, and savings banks --- makes ABA the largest banking trade association in the country.

Background

The Clinton Administration has been engaged for several years in an attempt to deal with the difficult issue of cryptographic export control policy. The Administration has acknowledged for many years that there are national and economic security justifications supporting their policy of licensing for export strong encryption products to support financial applications and, in fact, declared the financial system to be a "critical infrastructure."

The American Bankers Association applauded Vice President Gore's October 1996 statement announcing that the Clinton Administration was relaxing the export controls on some DES-BASED encryption products, and that controls on encryption used by financial institutions would also be further relaxed.

Historically, special provisions for financial institutions in cryptographic export control decisions have been embodied both in regulation and in long unwritten government practice. Specifically, the need for flexibility with respect to the application of export control regulations affecting financial institutions has long been recognized and accommodated by the National Security Agency (NSA), the State Department and the Department of Commerce .

On December 30, 1996, the Department published Interim-Final regulations implementing Executive Order 13026, transferring responsibility for export controls of dual-use encryption products to the Commerce Department and relaxing controls over certain encryption products that meet new requirements with respect to the recoverability of keys or content. The impact of the transfer of these regulations on financial institutions is the subject of this comment letter.

ABA Position

We are concerned that the interim-final regulations as published in the Federal Register do not reflect the flexibility of the prior International Traffic in Arms Regulation (ITAR) export process as previously practiced, the Administration's prior public statements promising to continue the favorable treatment of financial institutions' cryptographic export applications, or other understandings regarding additional liberalization arrived upon over a three-year period of discussions between the ABA and the Administration. The inclusion of such provisions can be easily justified as a matter of national and economic security. These Administration - acknowledged, but omitted policy statements and regulatory provisions would have, if incorporated in the regulation or otherwise formally documented, recognized the expansion of the rationale for the favorable treatment of cryptographic applications previously incorporated in the ITAR regulations under the "Money or Banking" exception as practiced and other long-established agency practices. Their inclusion would have provided written assurance to all concerned that the Administration's export control policy would neither impair the security of electronic banking and electronic commerce payments, nor impede the ability of U.S. intelligence and law enforcement agencies to pursue their missions.

Administration officials have insisted throughout the development of these regulations that it was not their intention to roll back "Money or Banking" or otherwise disadvantage financial institutions, instead their goal has been to update, and improve the export policy and procedures. Although the Vice President's October policy statement indicates that the Administration intends to continue to grant favorable treatment to banks' export applications (including permitting banks to export software and devices using longer key lengths) as a continuation of the policy, the Administration has yet to put such a new framework for financial institutions provisions in writing.

In the absence of a public document in sufficient detail to allay the concerns of the banking industry that the Administration's policy toward financial institutions' use of cryptography continues the previous policy and practice of the government as well as the ABA's cryptography policy developed in 1995, we must respond for the record to the regulations as published. We call upon the Bureau of Export Administration (BXA) and the Advisory Committee on Export Policy to act promptly to insure that the final regulations incorporate a financial institution policy that reflects previously favorable export policies and practices, and specifies the areas in which new accommodations for the requirements of financial institutions will permit new export options.

ABA has been urging a cryptography policy (adopted in August 1995, See attached) that would maximize the number of choices that banks and consumers would have to protect electronic commerce and banking via exportable cryptographic applications.

The Administration and members of Congress have supported the banking industry's effort to place strong cryptography into the hands of our customers around the world, so long as our applications do not impair domestic law enforcement and intelligence agency efforts to read criminals' and hostile' communications traffic. One complication for financial institutions participating in the debates over cryptographic export controls has been that some cryptographic technology boosters have made and continue to make unfounded statements that U.S. financial institution's domestic and international payments and information systems have been rendered insecure because of cryptographic export controls policies.

One result of this Administration's relaxation of export controls is the possibility of a practical increase in the baseline level of security of the network as general purpose products including 56 bit KMI and NON-KMI encryption and stronger KMI encryption are sold. KMI products represent another choice available to banks and their customers.

The financial services industry has made substantial progress in outlining a balanced policy framework that would permit license application-free export of "Limited-purpose" financial cryptographic applications, thus, setting us apart from supporters of elimination of all export controls. "Limited-purpose financial cryptographic applications" are implementations of cryptographic modules which would permit encryption, using very strong encryption algorithms and long key lengths, subject only to the requirement that the messages are in an approved payment format (credit card numbers, ABA routing numbers and account numbers, etc.) or general communications directed at U.S. banks. These applications could be implemented in either hardware or software and freely exported.

We request that the final regulations incorporate the changes suggested below as well as the necessary regulatory flexibility which would recognize the entire array of export arrangements which when incorporated into regulation would guarantee financial institutions and their customers the ability to use strong cryptography to secure electronic banking and commerce.

Rationale

The payment system is intrinsically interwoven with our national security and economic infrastructures. It is in the interest of all parties (government and industry) to have the payment system operate in a secure and efficient manner. Any opening or flaw in the security of the payment system compromises the integrity of all the participants in the system. Because transactions initiated by one bank or by a merchant will be settled by other banks, and because of the loss allocation mechanisms which would come into play in case of a failure to settle accounts, no one can rely on a system which lack's integrity by design.

Strong encryption and user authentication technology protects the interests of banks and their customers alike. These security mechanisms must be available to banks and their customers worldwide. The National Information Infrastructure will certainly fail to become a Global Information Infrastructure if consumers cannot access the full range of network services away from their homes. The U.S. payment system extends beyond our shores with points of presence wherever ATM and credit cards are accepted or U.S. financial institutions have branches or customers. Many U.S. financial institutions are providing worldwide remote access to electronic banking and commerce services to their commercial and retail customers. While many of the applications are proprietary, more and more of the mechanisms financial institutions use to communicate with customers are sold as over the counter mass market software.

Today, US financial institutions transfer approximately \$2.4 trillion a day by electronic means for the banks' own accounts and to settle customer initiated transactions. The volume of daily securities transfers dwarfs even these volumes. To secure this massive flow of funds and other value, banks have, for decades, used strong encryption in order to prevent payment related messages from being counterfeited, altered, or read by anyone other than authorized individuals.

How Banks Use Cryptography

Banks use cryptography for authentication and to protect the secrecy and integrity of information in transit. Much of the bank cryptography used for secrecy is designed to move data encrypted from point to point, rather than end to end. Data may be encrypted and decrypted several times as it moves across a network of networks. Thus, communications between or within banks and between banks and their customers are

generally encrypted only during transit. Which from the time of initial transmission until receipt by the recipient may typically be 1-2 seconds. In practice, a transaction would take the following steps: The financial institution receiving an encrypted transaction message would first decrypt and verify the authenticity and integrity of the sender and data, act upon the transmission, and then store the data in unencrypted form. Some types of stored data may be encrypted within the bank to protect the security and integrity of that data, however those systems include key management infrastructures managed by information security officers that guarantee access only by authorized personnel. When access to transaction data is needed, financial institutions are able to make the unencrypted plaintext of data available without a need to store or archive user or session keys. Financial institutions have been able to accommodate legitimate requests, subject of course to due process, for assistance without providing the government direct access to bank files, computer systems or encryption keys. There is no legitimate reason to change this relationship or to specifically mandate how performance should be effected.

Key Management Infrastructures in Banks

Banks employ encryption internally for system security and those uses are tightly controlled by information security officers. The key management infrastructures referenced above have been established to insure that encryption applications are used only by authorized personnel for authorized purposes, and that in the event that other authorized personnel need access to encrypted data, they can recover the keys and thus gain access to encrypted data.

The ABA's cryptography policy states that, **"we oppose government mandated key management systems for financial applications where keys would have to be stored outside the financial institution, (e.g. key registration/surrender or the mandatory escrow of cryptographic keys)." Further, we also oppose the application of rigid key management requirements including Supplement # 5 to part 742 of these regulations, that would impose unnecessary restrictions on the internal security decisions of financial institutions.** That banks should be able to hold their own keys or be able to choose a trusted third party is not at issue, however, it remains unclear how the "key recovery agent" requirements would be applied to financial institutions absent a financial institution specific section of these regulations. However the other issues are addressed, BXA should not have the right to approve or disapprove of a financial institution's internal key management infrastructure. We acknowledge that key recovery is a valuable technology that meet data storage requirements effectively and many banks may use key recovery "black box type" technology as part of their information security measures, but only at their option.

Compliance with Law Enforcement Requests for Assistance

Banks are accustomed to handling requests for assistance by law enforcement and there are established policies and procedures for handling even intelligence related (FISA) requests. The Right to Financial Privacy Act imposes requirements that banks provide available records to law enforcement authorities pursuant to legal process. Further, the funds transfer record keeping regulations impose requirements that certain information be included in wire transfers, that the information be recorded and stored so as to be recoverable following the presentation of a due process generated request by a law enforcement agency.

Why Bank Implementation of Cryptography Exceeds the Requirements

Because banks strictly control how the cryptographic tools they use internally as well as how the tools they transfer to customers are used, and because banks typically have the means to deliver plain text even absent a communications interception of financial transactions, and given the industry's long experience and legal mechanisms for complying with law enforcement requests, financial cryptography can be fairly characterized as recoverable and should be granted favorable treatment for export controls.

Technical Issues and Other Issues

Policies and Practices

Institutional knowledge of historic agency policies and practices held by employees of the NSA and the Department of State must be incorporated into the new regulatory policies and practices to be executed by the Department of Commerce.

Processing

While the majority of cryptography export applications will take far less time to process than under the previous policy, some financial institution export applications may, as a direct result of the new process, take longer to be receive approval than was previously possible and commonly experienced. We therefore urge that the export application review process be streamlined for financial applications. One approach to this would be for a number of agencies to grant delegations of authority to the NSA or Commerce. Commerce, NSA, and Justice can manage the minor questions that may arise from bank export applications. Alternatively financial applications could be handled under a new designation bridging the historic treatment of "money or banking" products and the new treatment of T.U. or KMI designated products.

Money or Banking

Interbank

One apparent oversight or drafting error is of special concern to our members and affects equipment used to effect inter-bank (high value) transactions. Specifically, the interim-final regulations as published abridge some of the language of the ITAR at Category XIII(B)(1)(ii) and thus do not completely transfer the "Money or Banking Exception." This in effect narrows the exception as a result of the omission of the prior reference in the ITAR to "equipment for the encryption of interbanking transactions." Under this exception, many financial hardware products and software applications automatically transferred to BXA without the need for a Commodities Jurisdiction request. This omission must be corrected.

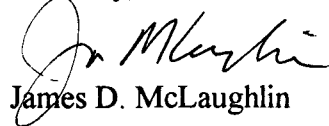
Retail

We would support extending the language of the "Money or Banking Exception" to include a new paragraph to be added to the Note at the end of ECCN 5A002, as follows:

"I. Cryptographic equipment or software specially designed, developed, or modified for use in conducting financial transactions provided that such equipment can be used solely to conduct financial transactions." It is critical that cryptographic applications (including CAPIs) for financial applications, where ever developed, be favorably provided for in this regulation , so long as they comply with the appropriate policies.

We are pleased to have the opportunity to file these comments and we look forward to working with the Department to develop a consistent set of regulations. If you have questions please contact Kawika Daguio (202-663-5434) or the undersigned.

Sincerely,



James D. McLaughlin

Attachment

American Bankers Association Policy Statement on Cryptography

ABA Policy on Cryptography

1. While the Data Encryption Standard (DES) might have a finite life span as a government certified standard because of non-technology agendas and reasons of strength, the financial services industry will continue to use DES based on risk assessment (e.g. value of the transaction) and the business application involved. At this time, the ABA believes that DES should be recertified for a minimum of ten years. In addition, any export controls on DES must be lifted.
2. A security framework encompassing a family of commercially available algorithms, including DES, should be developed. This framework must include a process for negotiated algorithm selection based on the level of risk and other business requirements. These algorithms must be available at a reasonable cost and free of unreasonable patent restrictions.

Characteristics of this family of algorithms include, but are not limited to:

- a. Alternatives that provide for high speed processing, as well as more complex algorithms that potentially take longer to encrypt information. In all cases, these must provide cost effective solutions.
- b. Availability in hardware (i.e. the encryption algorithm would be stored on a computer chip) and/or software (i.e. the algorithm would be a computer program that could be read into a computer from media, like a diskette and processed within the memory of the computer).
- c. Varying degrees of strength: the family should include some algorithms that are extremely sophisticated, ranging down to some that would be considered somewhat older and perhaps less sophisticated, such as DES. Sophisticated/complex algorithms would be used for applications that require a high level of security (funds transfer) and somewhat less sophisticated algorithms for lower dollar transactions (ATMs and credit cards).

d. A public\asymmetric key with products, such as RSA, that would provide the ability to "digitally sign" transactions and a private symmetrical algorithm key, such as DES, that would be used to encrypt information.

e. Developed, validated, and controlled in the private sector.

3. Due to the potential to negatively impact consumer confidence, consumer protection and privacy rights, we oppose government mandated key management systems for financial applications where keys would have to be stored outside the financial institution, (e.g. key registration/surrender or the mandatory escrow of cryptographic keys).

Further, any government encryption policy that is driven by "clipper type" escrow would impede the competitiveness of U.S. financial institutions in the global economy and electronic commerce.

Banks will continue to be responsible for key management and will continue to cooperate with government for law enforcement purposes, as required by law.

4. Export of cryptography for financial applications must not be restricted.
5. The establishment of U.S. policy for the commercial use of cryptography must include the full participation of Congress and the private sector, rather than be carried out solely by Executive Order.